МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский ядерный университет «МИФИ»»

# ЛАБОРАТОРНАЯ РАБОТА №1:
# «Поиск компонентов АСУ ТП в глобальной сети»

По предмету Информационная безопасность АСУ ТП

Выполнила студентка группы Б19-515
Щербакова Александра

Москва, 2022 г.

Задание 1.

*Описать, какие компоненты АСУ ТП возможно найти в глобальной сети. Какие особенности позволят их идентифицировать?*

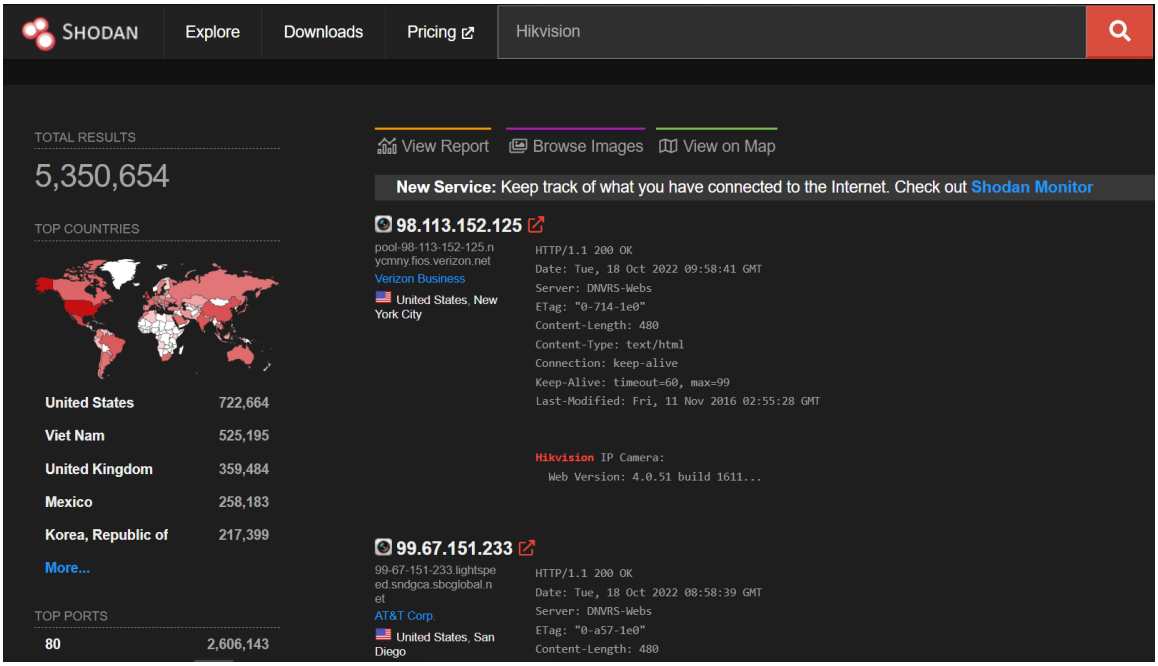
Ответ: Техническое и программное обеспечение.

Идентифицировать компоненты можно, например, по специфичным портам/протоколам или метаданным (вендор, модель, версия прошивки оборудования), которые отправляются в качестве ответа на запрос без аутентификации.

Задание 2.

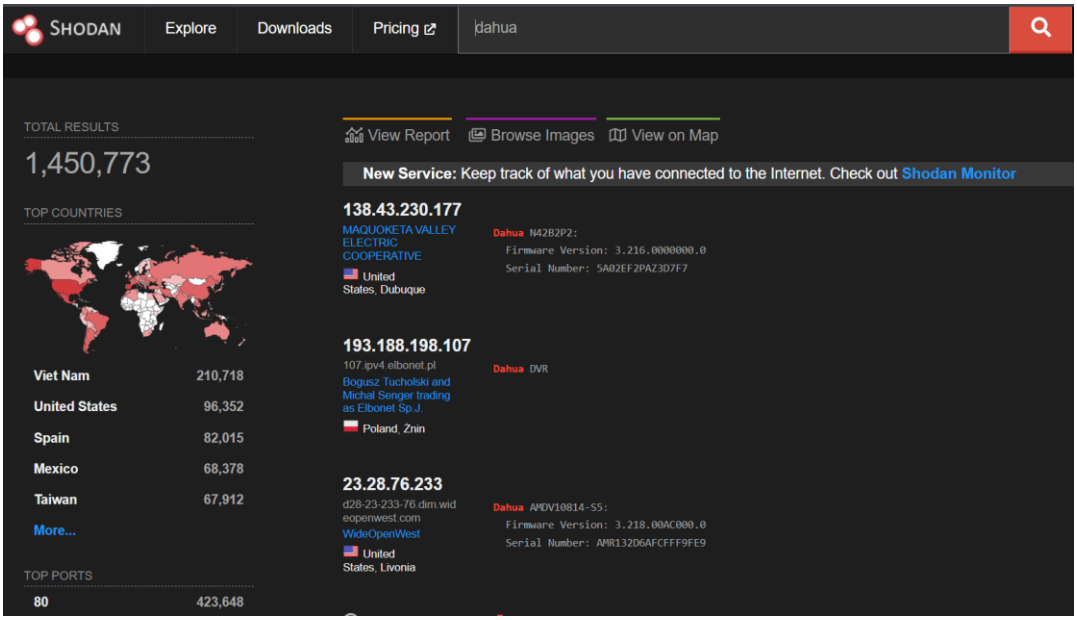
*Составить запросы для Shodan, которые позволят обнаружить компоненты АСУ ТП в глобальной сети. Объяснить, почему запросы составлялись таким образом. Число запросов — не менее 8 различных для разных компаний-производителей.*

1) Сравним количество оборудования, произведенного наиболее крупными вендорами видеонаблюдения в мире: Hikvision, Dahua, Axis Communications.
    1. Hikvision (Hangzhou Hikvision Digital Technology Co., Ltd.) — мировой лидер на рынке производства систем видеонаблюдения. Работает в 180 странах. Hikvision разрабатывает видеосистемы для всех сфер использования: частных домов, объектов бизнеса, управления дорожным движением, охраны дикой природы. Также производит охранные сигнализации, мониторы, домофоны, сетевое оборудование. Hikvision специализируется на технологиях IP и HD-TVI.



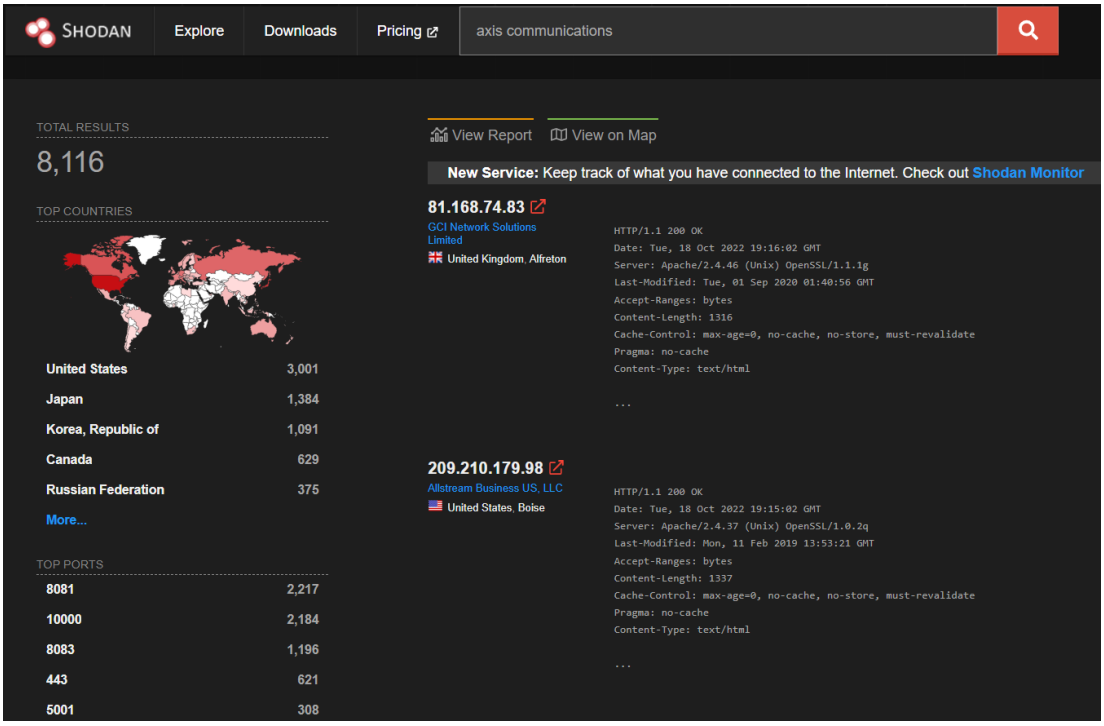
Итого более пяти миллионов устройств, страны с наибольшим распространением – США, Вьетнам, Великобритания. Наиболее часто используемый порт – 80.

2. Dahua (Zhejiang Dahua Technology Co., Ltd) — второй в мире производитель систем видеонаблюдения. Компания производит широкую линейку систем видеонаблюдения, а также охранные сигнализации, мониторы, дроны, домофоны, тепловизоры, видеорегистраторы и другие решения в сфере безопасности и автоматизации.



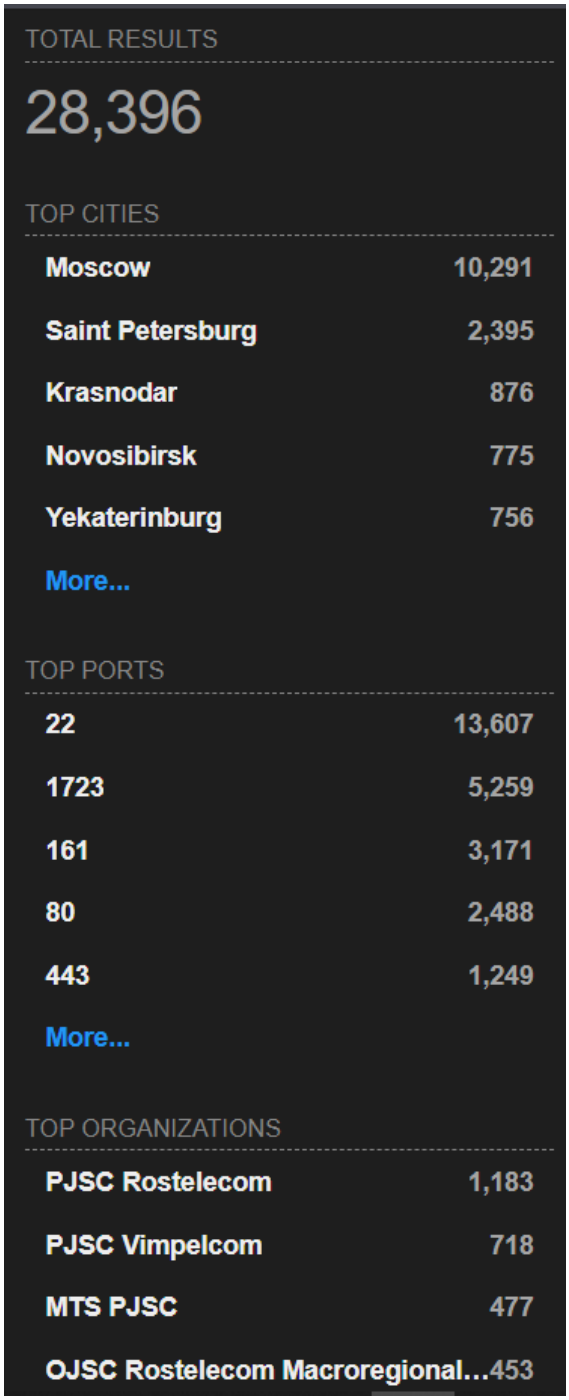

Почти полтора миллионов устройств, страны с наибольшим распространением – Вьетнам, США, Испания. Наиболее часто используемый порт – 80.

3. Axis Communications — один из крупнейших европейских производителей систем видеонаблюдения. Компания была инициатором перехода от аналоговых камер к IP-решениям. Axis стала первым в мире разработчиком видеосистем формата HDTV. Axis Communications производит системы видеонаблюдения для объектов любых типов, а также видеодомофоны, СКУД, видеосерверы и рабочие станции, программное обеспечение.



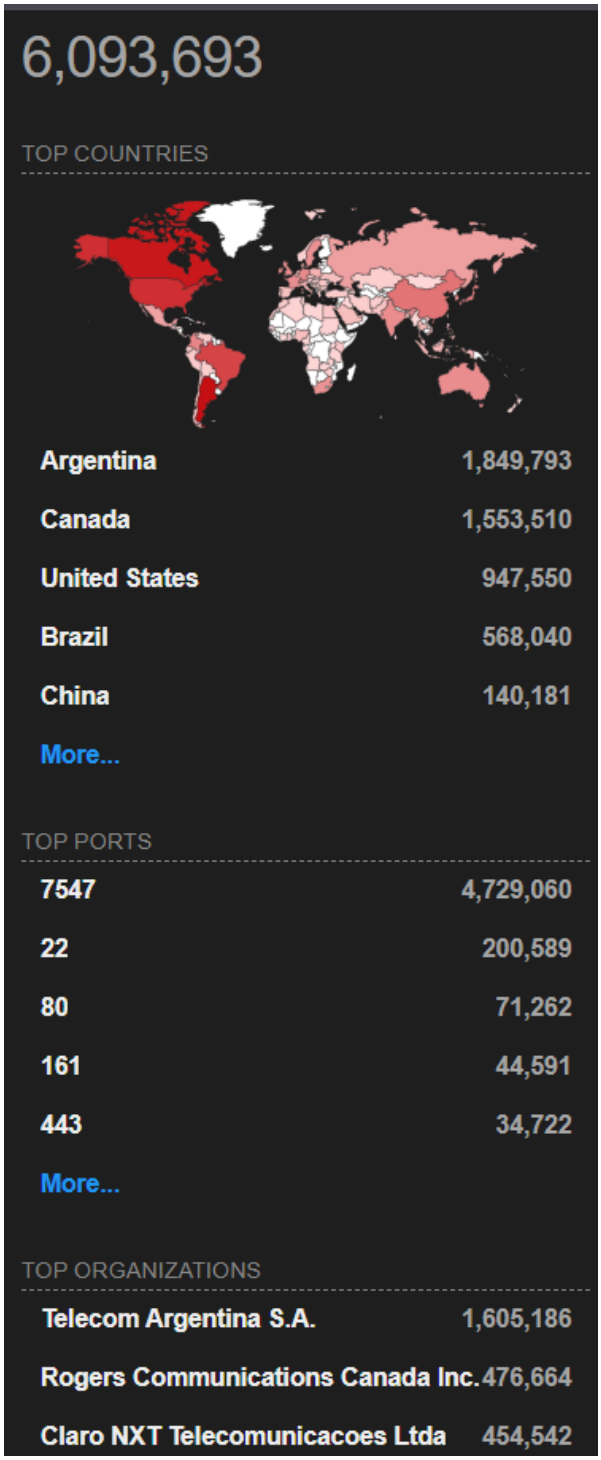

8 тысяч устройств, страны с наибольшим распространением – США, Япония, Корея. Наиболее часто используемый порты: 8081 и 8083 (стандартные протоколы HTTP сервисов), 10000 (NDMP протокол).

2) Cisco - американская транснациональная компания, разрабатывающая и продающая сетевое оборудование, предназначенное в основном для крупных организаций и телекоммуникационных предприятий.
   При помощи Shodan сравним, сколько устройств от вендора Cisco используют крупнейшая российская и зарубежная компании.
   Запрос: “cisco country:RU”




Всего в России около 28 тысяч устройств Cisco, наибольшая доля из них приходится на компанию Ростелеком: 1183 из них подключены к глобальной сети в данный момент.

Запрос: “cisco”

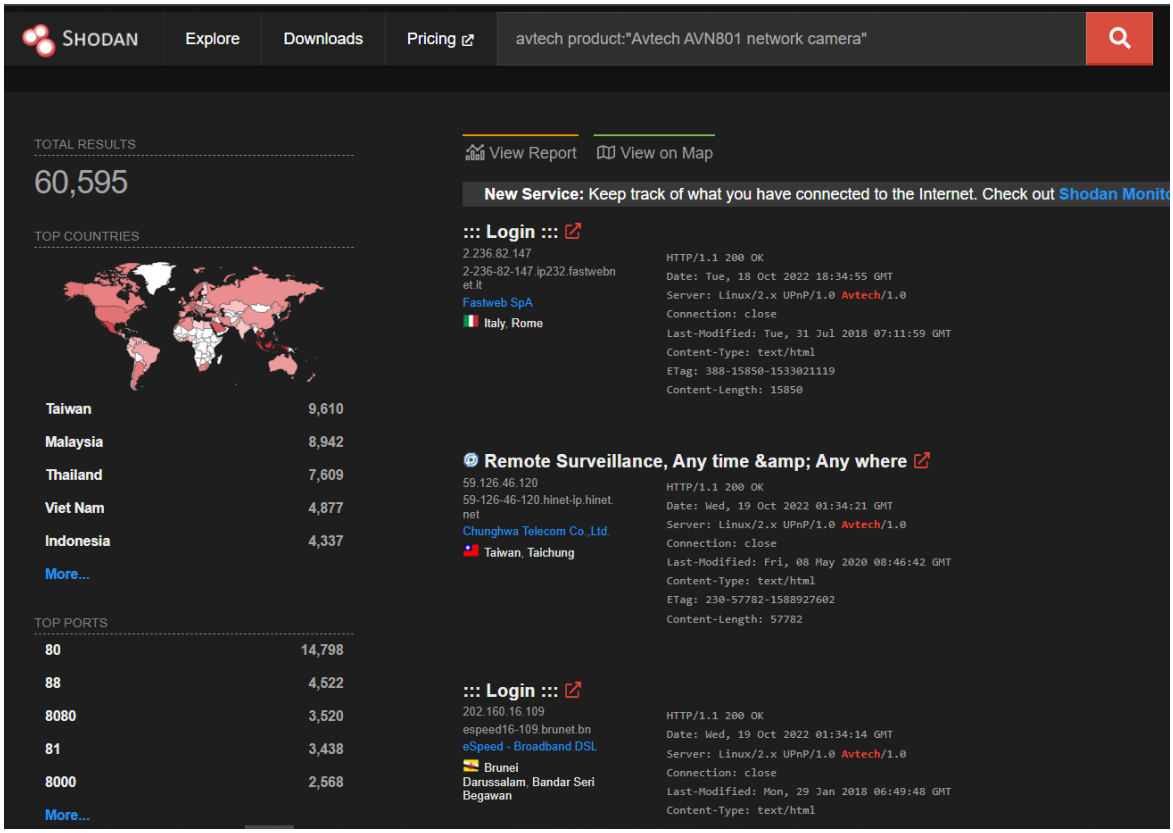



Всего в мире функционирует больше 6 миллионов устройств Cisco. Компания с наибольшая доля из них – Telecom Argentina S. A. – более полутора миллионов устройств (против 28 тысяч на всю Россию). Отчасти такое малое количество сетевых устройств в России можно связать с приостановлением деятельности Cisco в России.

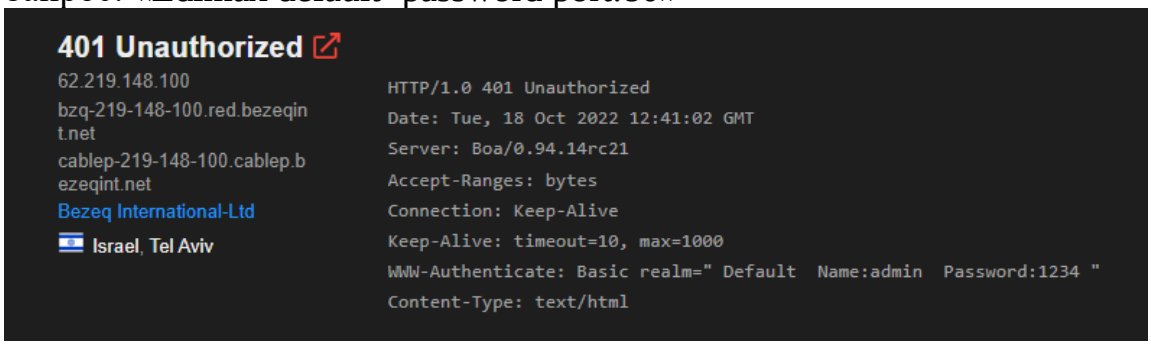
Кроме того, на скриншотах можно заметить преобладание порта 22 (стандартный порт для ssh соединения) в России и порта 7547 (CWMP сервис, используемый IoT-устройствами) в мире. Вероятно, это связано с бОльшим распространением Интернета вещей в мире, чем в России.

3) AVTECH — тайваньский бренд инновационных систем видеонаблюдения. В ассортименте этого производителя представлена продукция: DVR видеорегистраторы, IP-видеокамеры, сетевые видеорегистраторы, программное обеспечение и др.

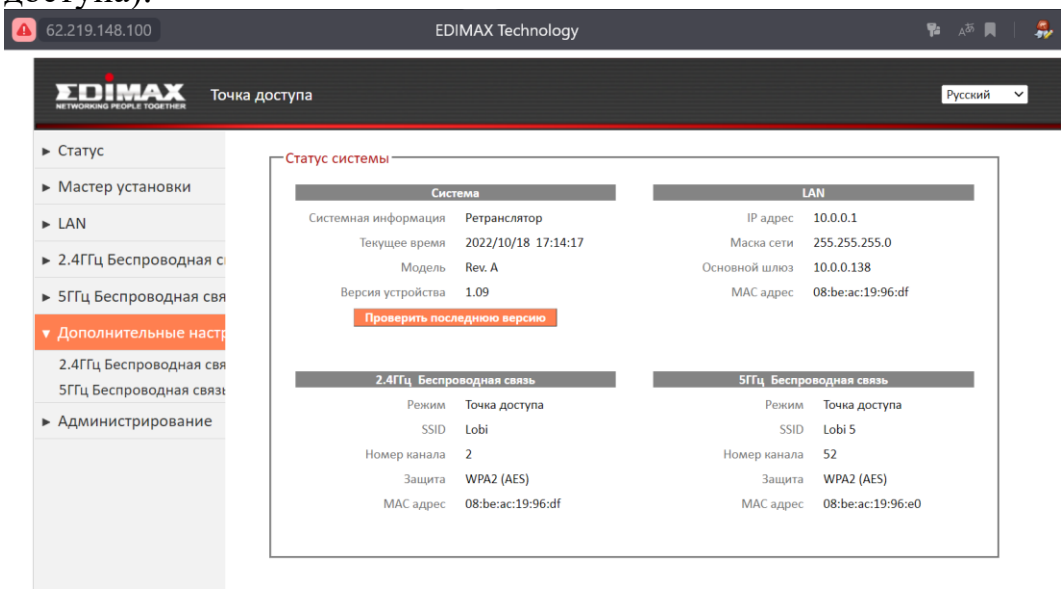
На примере вендора Avtech продемонстрируем возможность поиска в Shodan по названию устройства. Найдем, сколько в мире устройств Avtech AVN801 network camera (наиболее популярная модель от этого вендора) и через какие порты они подключены к глобальной сети.



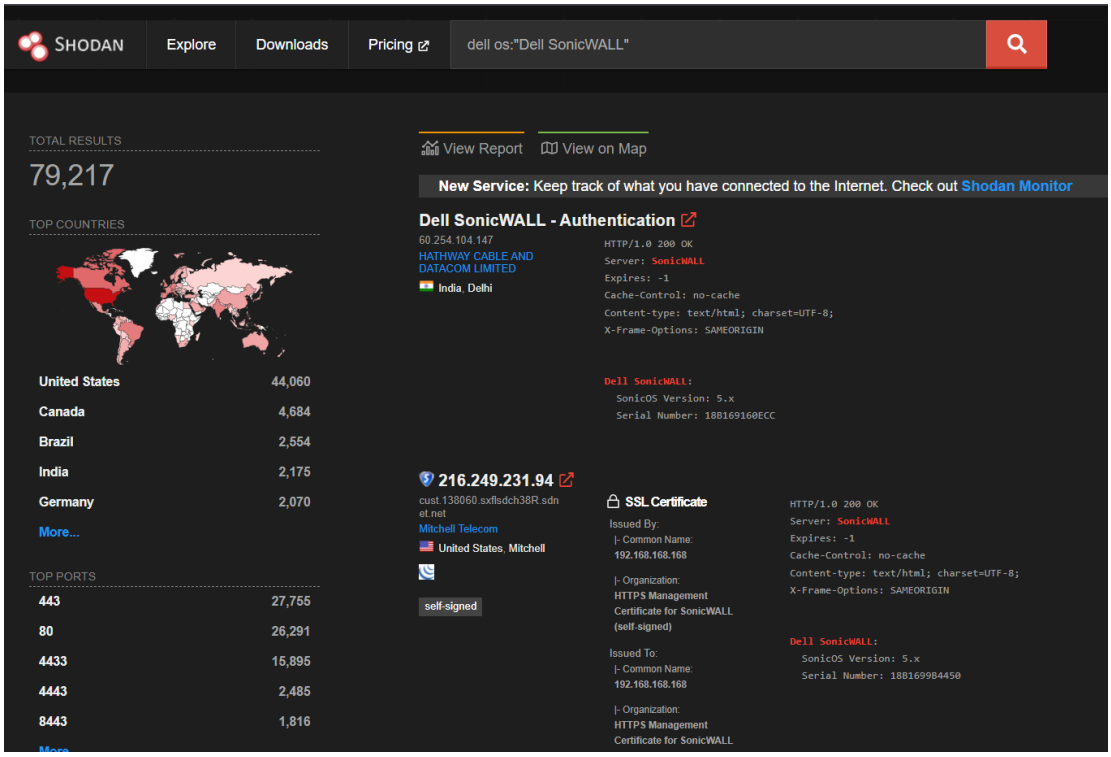

4) Edimax — мировой производитель сетевого и телекоммуникационного оборудования.
Многие администраторы сетевого оборудования не меняют стандартные аутентификационные данные. Как правило, этим «грешат» при установке IoT-устройств (например, видеокамер) или точек доступа.
На примере устройств от вендора Edimax получим доступ к устройству с дефолтным паролем. Будем искать по 80 порту (веб-клиенты HTTP).
Запрос: «Edimax default+password port:80»

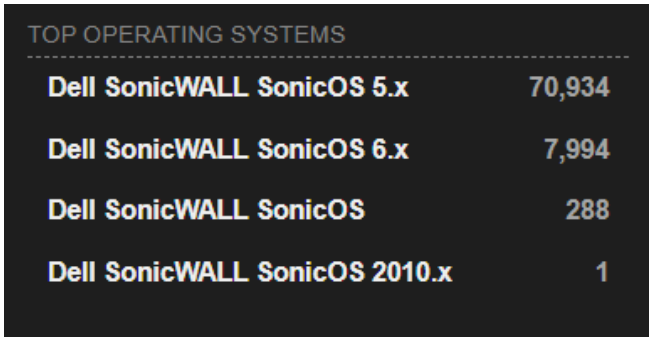


В баннере уже имеется информация о дефолтном пароле: Default Name:admin Password: 1234
Перейдя по ссылке и введя admin/1234, получаем доступ к устройству (это точка доступа):



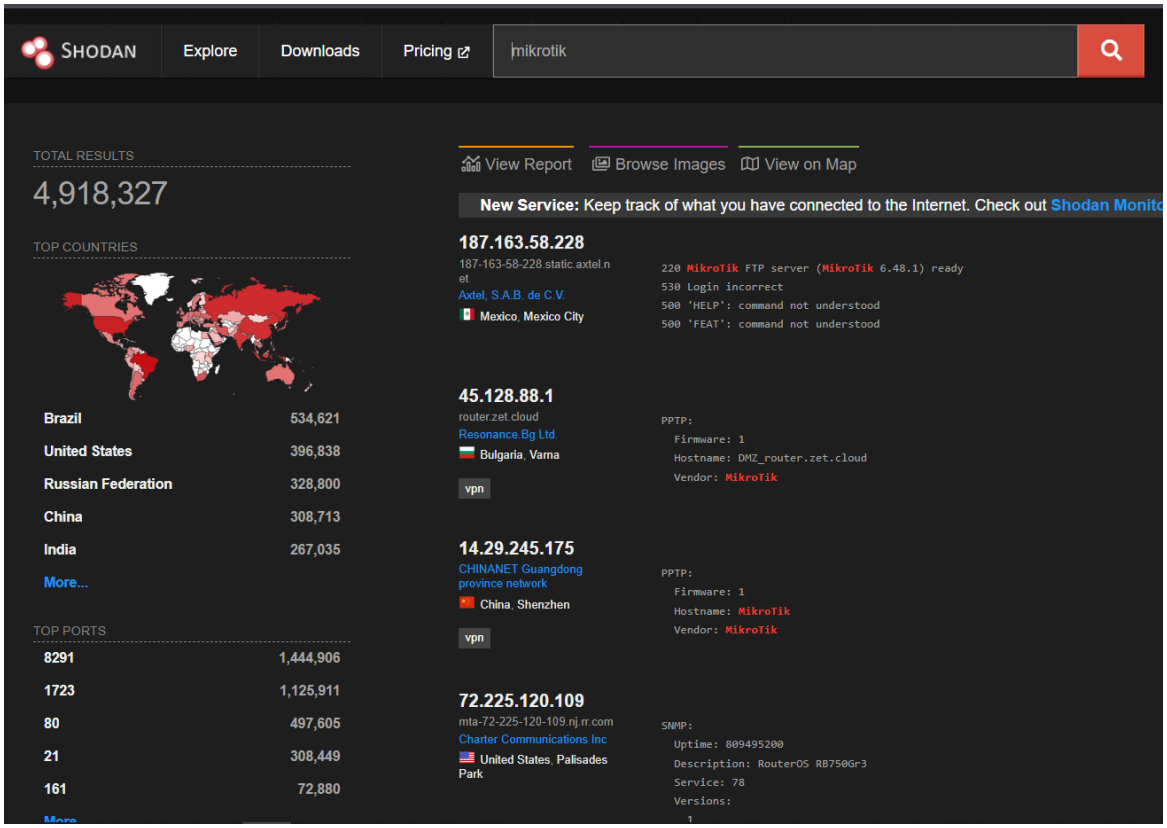

5) Dell — американская корпорация, одна из крупнейших компаний в области производства компьютеров. Компания Dell приобрела компанию SonicWALL в 2014 году. Продукция SonicWALL — это комплексные решения в области сетевой безопасности, безопасности электронной почты, безопасного удаленного доступа, защиты данных, анализа отчетности, централизованного управления и так далее.
При помощи Shodan можно выяснить, на каких операционных системах работает то или иное оборудование, так как версия прошивки часто записана в баннере. Для примера рассмотрим устройства от вендора Dell SonicWall.
Запрос: «dell os:”Dell SonicWall”»





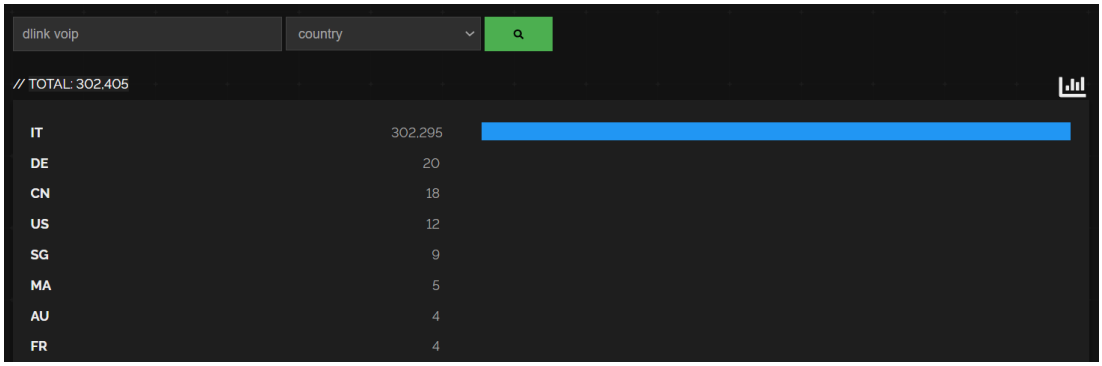

Абсолютное большинство устройств работает на версии ОС Dell SonicWALL SonicOS 5.x. Зная версию прошивки, злоумышленник может использовать уже известные уязвимости.

6) MikroTik - латвийский производитель сетевого оборудования, разрабатывает проводное и беспроводное сетевое оборудование, в частности маршрутизаторы, сетевые коммутаторы, точки доступа, а также программное обеспечение - операционные системы и вспомогательное программное обеспечение.

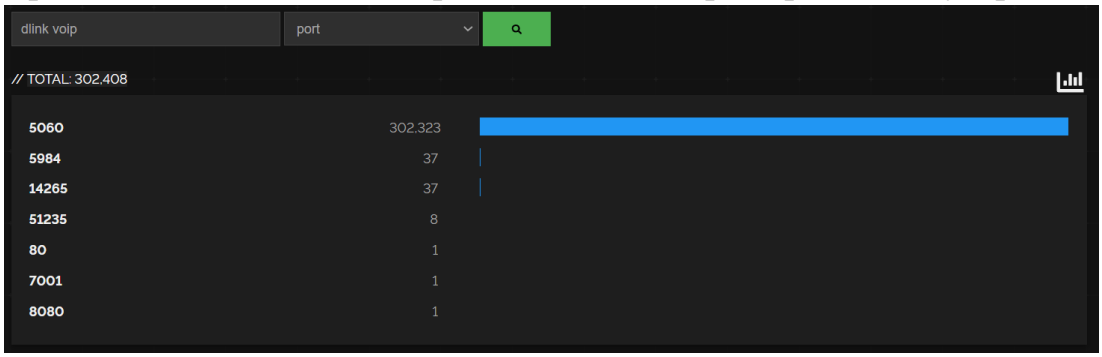



Можно заметить, что наибольшее число устройств функционирует на портах 8291 (стандартный TCP порт на MikroTik RouterOS для администрирования с Windows) и 1723 (PPTP протокол, один из VPN протоколов).

7) D-Link – мировой производитель сетевого и телекоммуникационного оборудования.
Найдем, в каких странах наиболее распространено использование оборудования D-Link для имплементации технологии VoIP. Как видно по диаграмме, эта технология используется только в Италии:




Кроме того, можно посмотреть, на каких портах работают устройства.

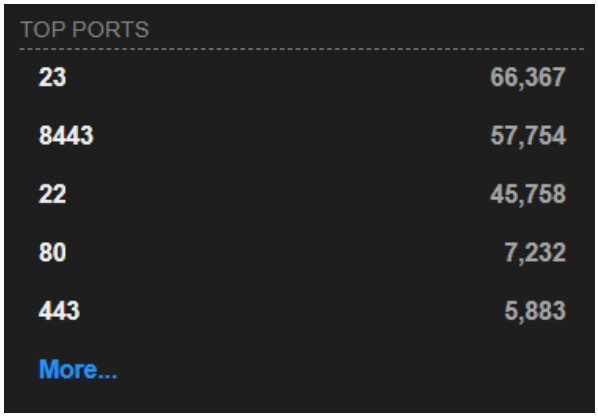



Результат запроса ожидаемый: порт 5060, так как он отвечает за протокол SIP, который и используется для ip-телефонии.

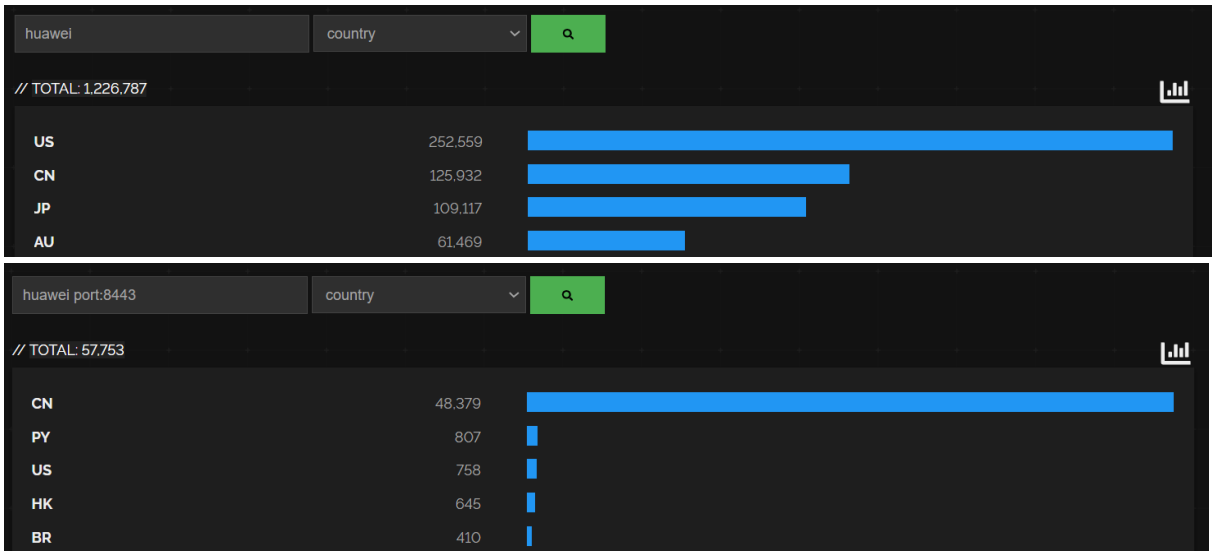
8) Huawei – китайская компания, одна из крупнейших мировых компаний в сфере телекоммуникаций. Среди продуктов уровня Enterprise компании Huawei можно найти современные серверы, системы хранения данных, коммутаторы, маршрутизаторы и другое оборудование
Посмотрим, на каких операционных системах работает оборудование Huawei в России.
Запрос: “huawei country:RU”


Абсолютное большинство устройств работают на ОС семейства Linux, а именно Linux Ubuntu версий 20.04 или 18.04.

Можно заметить, что наиболее используемые порты в устройствах Huawei – 23 (Telnet), 8443 и 22 (SSH):




Интерес вызывает порт 8443 – он отвечает за протокол RESTCONF (протокол для конфигурации и управления сетью, основанный на режиме REST, целью которого является предоставление стандартного механизма для веб-приложений для получения данных конфигурации, данных о состоянии и уведомлений о событиях). А именно, тот факт, что этот порт используется практически только в Китае, хотя оборудование Huawei распространено по миру более равномерно. Можно предположить, что использование порта 8443 является традиционным в Китае, в отличие от остальных стран.



**Заключение**

В лабораторной работе изучались базовые возможности сервиса Shodan. Сервис опрашивает порты устройств и на основе полученных в ответ баннеров выдает структурированную информацию и статистику по запросу.

Shodan позволяет обнаружить следующие мета-данные в баннерах: версии прошивки операционных систем устройств, названия модели продукта, сервер, типичные для вендора порты, и даже аутентификационные данные по умолчанию. Кроме того, можно подключиться к любым слабо защищенным портам (исключительно в ознакомительных учебных целях).

При помощи Shodan можно изучать статистику: количество оборудования, подключенного к глобальной сети в зависимости от страны/порта/компании/модели устройства/ОС и т.д..